Understanding the Sylow Theorems

Enlai Rooney

July 2024

Abstract

The Sylow Theorems are important results among those present in elementary group theory that describe the structure of groups. In this paper, we first go through the notion of group actions, and then provide proofs of the Sylow theorems. We finish by giving some applications of the theorems.

Contents

1 Introduction **1**

2 Group Actions **2**

3 The Sylow Theorems **3**

4 Applications **6**

1 Introduction

Group theory is an innately beautiful area of mathematics. One of the most elementary yet important results in group theory is Lagrange's Theorem, which appears in countless proofs of results of great significance. With this in mind, it seems reasonable to surmise that if the converse of Lagrange's Theorem were to be true, this would surely be a result of great utility too. Unfortunately, the converse is untrue. But this does not mean we should lose hope; while the converse lacks veracity, a partial converse of sorts could potentially be of just as much utility. The Sylow theorems are exactly this. They are a collection of theorems named after the Norwegian mathematician Peter Ludwig Sylow and are of particular use when attempting to classify finite groups. When the French mathematician Camille Jordan visited Christiania in 1872, he met with Sylow, who described to him what are now called "Sylow's theorems", which he had known since 1862.

2 Group Actions

In this section, we introduce group actions. In particular, we go through the notions of orbits and stabilizers and end with proofs of Cayley's theorem and the orbit-stabilizer theorem.

Definition 2.1 Let G be a group and X a set. An action of G on X is a homomorphism $\phi : G \to Sym(X)$.

Notation 2.2 Note that for some element $g \in G$ and some point $x \in X$, we denote the action of g on x by gx.

Definition 2.3 The orbit of a point $x \in X$ is the set of points to which x is transported by the action of G. That is, $Orb(x) = \{gx : g \in G\}$. The cardinality of an orbit is called its length.

Definition 2.4 The stabilizer of a point $x \in X$, denoted, $Stab(x)$, is the set of elements of G that keep x fixed when acting on it. That is, $Stab(x) = \{g \in G : gx = x\}$.

Definition 2.5 The transporter from x to y is the set of elements that send x to y. That is, $Trans(x, y) = \{g \in G : gx = y\}$.

Theorem 2.6 $\forall x \in X, Stab(x) \leq G$.

Proof. Firstly, we note that the identity is in $Stab(x)$ as it is in the kernel of the associated homomorphism. For any $g, h \in Stab(x)$, $(gh)x = g(hx) = gx = x$ which shows that $Stab(x)$ is closed under multiplication. Also, $x = (g^{-1}g)x = g^{-1}(gx) = g^{-1}x$ which shows that the inverse of every element in $Stab(x)$ is also in $Stab(x)$. Thus, $Stab(x) \leq G$. ■

Theorem 2.7 *The orbits of X form a partition.*

Proof. We firstly note that every point in X is clearly in its own orbit. Now, we wish to prove that if two orbits overlap, they must be the same orbit. Consider some $x \in Orb(y) \cap Orb(z)$. We know that $x = gy = hz$ for some $g, h \in G$. Thus, if $w = mz$ for some $m \in G$, then $w = mh^{-1}x = mh^{-1}gy$. Thus $Orb(z) \subset Orb(y)$. By an analagous argument, we also have that $Orb(y) \subset Orb(z)$, implying that the two orbits must be the same. ■

Definition 2.8 An action is:

1. Faithful if the kernel of the associated homomorphism is trivial
2. Transitive if there's only one orbit
3. Regular if it is both faithful and transitive

Theorem 2.9 (Cayley) *Every group of order n is isomorphic to some subgroup of S_n.*

Proof. We consider the action of G on itself by left multiplication where G is some group of order n. It is clear to see that this action is faithful, and so by the first isomorphism theorem, G must be isomorphic to the image of the homomorphism $\phi : G \to Sym(G)$ which, since $Sym(G) \cong S_n$, is a subgroup of S_n. ■

Theorem 2.10 (Orbit-Stabilizer) *Let G be a group acting on X. Then for any point $x \in X$,*

$$|G| = |Stab(x)||Orb(x)|.$$

Proof. Due to Lagrange's Theorem, what we want to prove is equivalent to proving that $|Orb(x)| = [G : Stab(x)]$. We will proceed by proving this statement. We define a mapping $\phi : Orb(x) \to G/Stab(x)$ by $\phi(gx) = gStab(x)$. We first show that ϕ is well-defined and injective. Consider $g_1, g_2 \in G$ such that $g_1x = g_2x \in Orb(x)$. This implies that $(g_2^{-1}g_1)x = x \iff g_2^{-1}g_1 \in Stab(x)$, which is equivalent to $g_1Stab(x) = g_2Stab(x)$. Thus $g_1x = g_2x$ if and only if $\phi(g_1x) = \phi(g_2x)$, and so we see that ϕ is well-defined and injective. It's clear that ϕ is surjective since for any $gStab(x) \in G/Stab(x)$, we have that $\phi(gx) = gStab(x)$. Thus ϕ gives a one-to-one correspondence between the elements of $Orb(x)$ and the left cosets of $Stab(x)$ in G, so $|Orb(x)| = [G : Stab(x)]$ as desired. ■

3 The Sylow Theorems

Definition 3.1 Let G be a finite group of order p^nm where $p \nmid m$. A Sylow p-subgroup of G is one of order p^n.

Lemma 3.2 *If $p \nmid m$, then $p \nmid \binom{p^rm}{p^r}$.*

Proof. We have that

$$\binom{p^rm}{p^r} = \frac{(p^rm)!}{(p^r)!(p^rm - p^r)!} = \frac{p^rm(p^rm-1)...(p^rm-p^r+1)}{(1)(2)...(p^r-1)(p^r)}$$

That is,

$$\binom{p^rm}{p^r} = m\prod_{i=1}^{p^r-1}(\frac{p^rm-i}{i})$$

Let us consider $\frac{p^rm-i}{i}$ for some $1 \leq i < p^r$. If $p^j|i$ then $j < r$ and $p^j|(p^rm-i)$. Similarly, if $p^j|(p^rm-i)$, then $j < r$ and $p^j|i$. Thus for each $\frac{p^rm-i}{i}$, the numerator is divisible by p^j if and only if the denominator also is. Thus each fraction in the product is clearly non-zero modulo p and so we are done. ■

Lemma 3.3 *Let G be a group acting on a set of sets Ω and let $\omega \in \Omega$ be a subset of G. Then $|Stab(\omega)|$ divides $|\omega|$.*

Proof. We define $H := Stab(\omega)$. Since $H\omega = \omega$, we have that for all $\psi \in \omega$, $H\psi \subset \omega$. Hence for all $\psi \in \omega$, the corresponding right coset of H is a subset of ω. This implies that the right cosets of H partition ω, and since the cosets have the same size, we have that $|H|$ divides $|\omega|$. ■

Theorem 3.4 (Sylow's First Theorem) *If G is a group and p a prime such that $p \mid |G|$, then there exists a Sylow p-subgroup of G.*

Proof. We'll let $|G| = p^n m$ where $p \nmid m$ and denote the set of all subsets of G with order p^n by Ω. Firstly, it's quite clear that $|\Omega| = \binom{p^n m}{p^n}$. Now, we let G act on Ω by left multiplication. Given that Ω is partitioned by its orbits, the sum of the lengths of the orbits is equal to $|\Omega|$. By Lemma 3.2, we have that p doesn't divide $|\Omega|$ and thus there must be at least one orbit whose length is coprime to p. We choose $\omega \in \Omega$ such that its orbit satisfies this; that is, $p \nmid |Orb(\omega)|$.
We now consider $Stab(\omega)$.
By the Orbit-Stabilizer theorem, we know that $|Stab(\omega)||Orb(\omega)| = p^n m$. Since $p \nmid |Orb(\omega)|$, it must be that $p^n \mid |Stab(\omega)|$. But due to Lemma 3.3, we must also have that $|Stab(\omega)| \mid p^n$. It follows that $|Stab(\omega)| = p^n$ and so Given that $Stab(\omega) \leq G$, we see that $Stab(\omega)$ is our desired Sylow p-subgroup. ■

Definition 3.5 Let H and K be two subgroups of G. Then H and K are said to be conjugates if there exists some $g \in G$ such that $H = gKg^{-1}$.

Lemma 3.6 *Let G be a group of order p^n and let X be a finite set. Then $|X| \equiv |X^g| \pmod{p}$ where X^g denotes the set of points of X that are fixed by every $g \in G$.*

Proof. Consider a set of representatives $x_1, ..., x_n \in X$ for the G-orbits of X. That is, elements $x_1, ..., x_n \in X$ such that no two x_i are in the same G-orbit of X and the orbits of each x_i collectively make up all of the G-orbits of X. We know that $|X| = \sum_{i=1}^{n} |Orb(x_i)|$. Due to the orbit-stabilizer theorem, we know that $|Orb(x_i)|$ must be a factor of $|G| = p^n$ for all $1 \leq i \leq n$. If x_i isn't fixed by every $g \in G$, then $|Orb(x_i)| > 1$ and thus must be some power of p; crucially, it is $0 \pmod{p}$. If x_i is fixed by every $g \in G$, then $|Orb(x_i)| = 1$, and so for every x_i fixed by every $g \in G$, the sum $\sum_{i=1}^{n} |Orb(x_i)|$ increases by 1 modulo p. The result follows. ■

Theorem 3.7 (Sylow's Second Theorem) *For a given prime p and some group G, all Sylow p-subgroups of G are conjugate.*

Proof. Let G be a group of order $p^n m$ with p prime where $p \nmid m$ and let H be a Sylow p-subgroup of G.We consider the set $X = G/H$, the left cosets of H. By definition, $|X| = [G : H] = m$. Let K be another Sylow p-subgroup of G. We now let K act on X by left multiplication. By lemma 3.6, the number of fixed points of G/H under the action of K is congruent to $[G : H]$ mod p. Since $[G : H] \equiv m \not\equiv 0 \pmod{p}$, there must be at least one point that is fixed under the action. We will denote one of these fixed points by gH. We have $kgH = gH$ for all $g \in G$. This implies that $g^{-1}KgH = H \Rightarrow g^{-1}Kg \subset H$. Because $g^{-1}Kg$

and H are finite sets of the same size, the inclusion implies equality and we thus have that the two groups are conjugate. ■

Corollary 3.8 *A Sylow p-subgroup of G is unique if and only if it is normal in G.*

Proof. If a Sylow p-subgroup is unique then it is equal to all of its conjugations and thus must be normal. If there are multiple Sylow p-subgroups then they must be conjugate to each other. This means they are not closed under conjugation and so can't be normal. ■

Remark 3.9 Note that corollary 3.8 means that the Sylow p-subgroups of abelian groups must be unique.

Definition 3.10 Let G and H be groups such that $H \leq G$. Then the normalizer of H in G, denoted by $N(H)$, is the set $\{g \in G : gHg^{-1} = H\}$.

Lemma 3.11 *Let H and G be groups such that $H \leq G$. Then $H \subseteq N(H) \leq G$. Also, if $H \leq K \leq G$, then $H \trianglelefteq K$ if and only if $K \leq N(H)$.*

Proof. Take any $h \in H$. Then for any $c \in H$, we have that $h^{-1}ch \in H$, so $h^{-1}Hh \leq H$. Also, $h^{-1}(hch^{-1})h = c$, and $hch^{-1} \in H$. Thus we see that every element of H is in $h^{-1}Hh$, so $H = h^{-1}Hh$ and $H \subseteq N(H)$. Note that this implies that $e \in N(H)$. Now, take any $a, b \in N(H)$. Then $(ab)^{-1}Hab = b^{-1}(a^{-1}Ha)b = b^{-1}Hb = H$ and so $N(H)$ is has closure. Also, $a^{-1}Ha = H \Rightarrow H = aHa^{-1}$. That is, $(a^{-1})^{-1}Ha^{-1} = H$ and hence $a^{-1} \in N(H)$.
Now for the second part. By the defintion of a normal subgroup, we know that $H \trianglelefteq K \iff k^{-1}Hk = H$ for all $k \in K$. But by the definition of $N(H)$, we see that this only occurs when $K \leq N(H)$. ■

Theorem 3.12 (Sylow's Third Theorem) *Let G be a group of order $p^n m$ where p is prime and $p \nmid m$. If the number of Sylow p-subgroups of G is denoted by $n_p(G)$ then:*

1. $n_p(G) \equiv 1 \pmod{p}$
2. $n_p(G) \mid m$
3. *if P is some Sylow p-subgroup of G, then $n_p(G) = [G : N(P)]$*

Proof of part 1 of Sylow's Third Theorem. We define S to be the set of all Sylow p-subgroups of G. We consider a particular Sylow p-subrgoup P and let it act on S by conjugation. S must be finite since G is finite and thus, by lemma 3.6, we have that $|S| = n_p(G) \equiv |S^P| \pmod{p}$. Due to lemma 3.11, we know that $P \subseteq N(P)$. That is, P is closed under conjugation by one of its elements, and so is a fixed point under the action. We now consider some other fixed point, which we'll refer to as Q. As $pQ = Qp$ for all $p \in P$, it follows that $P \subseteq N(Q)$. Again using lemma 3.11, we know that $Q \subseteq N(Q)$, and thus, $P, Q \leq N(Q)$. By Lagrange's theorem, $p^n \mid |N(Q)|$, and as $p^{n+1} \nmid |G|$, we also

have that $p^{n+1} \nmid |N(Q)|$. And so we see that N and Q are Sylow p-subgroups of $N(Q)$ which, by Sylow's second theorem, means that they must be conjugate in $N(H)$. By lemma 3.11 again, we know that $Q \trianglelefteq N(Q)$ but in light of corollary 3.8, this means that $P = Q$. And so we see that there is only a single fixed point in S, this implying that $n_p(G) \equiv 1 \pmod{p}$. ■

Proof of part 2 of Sylow's Third Theorem. We now consider the action of G on S by conjugation. We know that Sylow p-subgroups of G are conjugate and so their can only be a single orbit of length $n_p(G)$. By the orbit-stabilizer theorem, it follows that $n_p(G) \mid |G| = p^n m$. Given that $n_p(G) \equiv 1 \pmod{p} \Rightarrow gcd(n_p(G), p) = 1$, it must be that $n_p(G) \mid m$. ■

Proof of part 3 of Sylow's Third Theorem. We again inspect the action of G on S. By the orbit-stabilizer theorem, $n_p(G) = [G : Stab(P)]$. Since the action is conjugation, we know that $Stab(P) = N(P)$, and so the result follows. ■

4 Applications

In this section, we give some simple applications of the Sylow theorems.

Theorem 4.1 (Cauchy's Theorem) *Let G be a finite group and be a prime number such that p divides $|G|$. Then G has an element of order p.*

Proof. By the first Sylow theorem, G has a Sylow p-subgroup P, the order of which is p^n, for some $n \in \mathbb{Z}^+$. Take any $e \neq a \in P$. By Lagrange's Theorem, $|a| = p^k$ for some $1 \leq k \leq n$. But then $|a^{p^{k-1}}| = p$. ■

Definition 4.2 We say that a group is simple if it is nontrivial and has no nontrivial proper normal subgroups.

Theorem 4.3 *There are no simple groups of order* 20.

Proof. Let G be a group with order 20. By the first Sylow theorem, there exists one or more Sylow 5-subgroups in G and by the third Sylow theorem, the number of such subgroups is congruent to 1 (mod 5) and must divide 4. The only possible such number is 1. Thus by corollary 3.8, this Sylow 5-subgroup is normal, and so G cannot be simple. ■

Theorem 4.4 *There are no simple groups of order* 56.

Proof. Let G be a group of order 56. By the first Sylow theorem, there exists one or more Sylow 7-subgroups in G and by the third Sylow theorem, the number of such subgroups is congruent to 1 (mod 7) and divides 8. The only possible such numbers are 1 and 8. If there's only a single Sylow 7-subgroup then by corollary 3.8 it must be normal and we are done. So let us assume that there are 8 Sylow 7-subgroups. Each of these subgroups must be cyclic and thus their intersection must be trivial. This leaves $8 \times 6 = 48$ distinct elements in the group, each of order 7.

Now let us consider the Sylow 2-subgroups of G. By similar reasoning, we see that there are either one or seven. Any element of a Sylow 2-subgroup must have as its order a power of 2 and therefore cannot be one of the 48 elements of order 7 in the Sylow 7-subgroups. Since a Sylow 2-subgroup has order 8, there is only enough room for a single Sylow 2-subgroup in a group of order 56, and thus this single Sylow 2-subgroup must be normal by corollary 3.8. ■

Theorem 4.5 *Let G be a group of order pq where p and q are primes such that $p < q$. Then the Sylow q-subgroup of G is normal. In particular, G is not simple.*

Proof. By the third Sylow theorem, the number of Sylow q-subgroups is of the form $kq + 1$ for some $k \in \mathbb{Z}$ such that $(kq + 1)|p$. Since $q > p$, it must be that $k = 0$ and thus there is only one Sylow q-subgroup. By corollary 3.8, it follows that this Sylow q-subgroup is normal. ■

Theorem 4.6 *Let G be a group of order pqr where p, q and r are distinct primes. Then G is not simple.*

Proof. WLOG, let us say that $p < q < r$. Then, by the third Sylow theorem, the number of Sylow r-subgroups is of the form $kr+1$ where $k \in \mathbb{Z}$ and $(kr+1)|pq$. The only positive divisors of pq are $1, p, q$ and pq but we cannot have that $kr + 1 = p$ or q since this contradicts $p < q < r$, and if $kr + 1 = 1$ then we are done; so let us assume that there are pq Sylow r-subgroups. Now, all of these subgroups must have prime order and thus intersect trivially, giving us $pq(r-1)$ elements of order r.
Now let's consider the Sylow-q subgroups of G. We similarly have that there are $lq + 1$ such subgroups where $l \in \mathbb{Z}$ and $(lq + 1)|pr$. Since $q > p$, we cannot have that $lq + 1 = p$ and if $lq + 1 = 1$ then we are done; so let us assume that there are r or pr such subgroups. In either case, we have that there are at least r Sylow-q subgroups and thus there must be at least $r(q - 1)$ elements of order q.
Finally, the number of Sylow p-subgroups is $mp+1$ where $m \in \mathbb{Z}$ and $(mp+1)|qr$. If $mp + 1 = 1$ then we are done, so let us assume that there are at least q Sylow p-subgroups. Thus there are at least $q(p - 1)$ elements of order p. Adding in the identity, we have that there must be at least

$$pr(q - 1) + r(q - 1) + q(p - 1) + 1 = pqr + qr - q - r + 1 > pqr + qr - 2r + 1$$

elements since $q < r$. But since $q > p$ and p is prime, we know that $q \geq 3$, so $qr \geq 2r$. Thus we have that there must be at least $pqr + 1$ elements which is a contradiction. ■

Theorem 4.7 (Wilson's Theorem) *A natural number p is prime if and only if* $(p - 1)! \equiv -1 \pmod{p}$.

Proof. We will only provide a proof of the "only if" part, since it can be done with the Sylow theorems. We consider the symmetric group S_p for some prime

p. Since $p|p!$ but $p^2 \nmid p!$, we see that the Sylow p-subgroups of S_p are cyclic groups of order p. Now, there are $(p-1)!$ p-cycles in S_p and every Sylow p-subgroup contains $(p-1)$ such cycles. Hence there are $\frac{(p-1)!}{p-1} = (p-2)!$ Sylow p-subgroups and thus, by the third Sylow theorem,

$$(p-2)! \equiv 1 \pmod{p}$$

$$\Rightarrow (p-1)! \equiv p-1 \equiv -1 \pmod{p}$$

■